XMSS: Extended Hash-Based Signatures

draft-irtf-cfrg-xmss-hash-based-signatures

A. Hülsing, D. Butin, S.-L. Gazdag, A. Mohaisen
Hash-based Signature Schemes

[Mer89]

Only secure hash function
Security well understood
Post quantum
Fast

FIG 1
AN AUTHENTICATION TREE WITH N = 8.
Security

- Intractability assumption
- Cryptographic hash function
- Digital signature scheme
Security

- Intractability assumption
- Cryptographic hash function
- Digital signature scheme
Post-Quantum Security

n-bit hash function

Grover‘96:

Preimage finding $O(2^n) \rightarrow O(2^{n/2})$

Brassard et al. 1998:

Collision finding $O(2^{n/2}) \rightarrow O(2^{n/3})$

Aaronson & Shi’04:

Quantum collision finding $2^{n/3}$ is lower bound
Advanced Applications

• Forward Secure Signatures
  • Security of old signatures after key compromise

• Delegatable / Proxy Signatures
  • Securely delegate signing rights

→ Require specific pseudorandom key gen
Design Choices

• Follow literature as close as possible
• Full collision-resilience
• Classical and post-quantum secure parameters
• Prepared for stateless schemes (SPHINCS)
Schemes in the Draft

• Winternitz One Time Signature (WOTS$^+$)

• Extended Merkle (tree) signature scheme (XMSS)

• Multi-tree XMSS (XMSS$^{^\text{MT}}$)
Conclusion

• Draft is out


We want your feedback!